REMARKS

Applicants respectfully request favorable reconsideration of this application, as amended.

Claims 1-4 and 6-17 are pending. By this Amendment, Claims 6-11 have been amended to more clearly recite the subject matter intended to be claimed. Claims 8-11 have also been amended to clarify the classification to which the claimed subject matter is directed. Claims 12-17 have also been amended for consistency.

In the Office Action, Claims 8-17 were rejected under 35 U.S.C. § 101 as being allegedly directed to non-statutory subject matter; and Claims 1-4, 6-8 and 12-17 were rejected under 35 U.S.C. § 112, first paragraph, as allegedly not enabled.

Rejection Under 35 U.S.C. § 101

Without acceding to the rejection under § 101, Claims 8-11 have been amended to more clearly recite the subject matter intended to be claimed.

For example, Claim 8 now recites, *inter alia*, one or more computer readable storage media upon which is encoded and stored a sequence of programmable instructions which, when executed by one or more processors, cause the processors to: communicate to a server machine a certificate of a user which is sent by a client machine via a security module, insert said certificate unmodified into a cookie header, and transmit the request, including said cookie header containing said unmodified certificate, from the security module to the server machine.

Therefore, Applicants respectfully submit that Claim 8 recites structural and functional interrelationships between the instructions and the functions being performed by one or more processors and, further, also recites that the instructions are

encoded and stored one or more computer readable storage media. Therefore, Applicants respectfully submit that Claim 8 is directed to statutory subject matter. MPEP § 2106.01; See *In re Warmerdam*, 33 F.3d 1354, 1360-61 (Fed. Cir. 1994).

Claims 9-11, which depend from Claim 8, have also been amended to recite computer-readable storage media.

The rejection under § 101 with respect to Claims 12-17 is not understood. Claims 12-14 are directed to a system, and claims 15-17 are directed to an apparatus. Therefore, Claims 12-17 are clearly directed to statutory subject matter.

Accordingly, Applicants respectfully request that the rejection under § 101 be withdrawn.

Rejection Under 35 U.S.C. § 112, First Paragraph

Regarding the rejection under § 112, with respect to Claims 1-4 and 8-11 this rejection is respectfully traversed. Applicants' claimed security module is described in detail in various portions of Applicants' disclosure. For example:

> "[0029] In the system 1, the security module 2c handles a security protocol. The security module 2c is in the form of a machine 2 (embodiment illustrated) or a software module integrated into a machine 2 such as the server machine 2b."
>
> "[0030] In the embodiment of the invention illustrated in FIG. 1, the security module 2c is an intermediate machine 2. The security module 2c, called a security or front-end box, is split off upstream from the server machine 2b."
>
> "[0031] The security module 2c makes it possible to handle a security protocol such as SSL or TLS or an equivalent protocol. A protocol equivalent to the SSL or TLS protocol is a protocol that makes it possible to authenticate the user 4 by means of a certificate. The security module 2c makes it possible to transmit a certificate from the client machine 2a to the server machine 2b."
>
> "[0032] The security module 2c includes analyzing means 6 that

make it possible to request a certificate of the user 4 from the client machine 2a, retrieve the certificate of the user 4 requested from the client machine 2a and send it to the server machine 2b. In the embodiment illustrated, the analyzing means are in the form of a software module integrated into the security module 2c."

"[0033] The certificate from the client machine 2a requested by the server machine 2b during the mutual authentication of the SSL protocol is transmitted from the client machine 2a to the security module 2c. Since the SSL protocol is not implemented between the security module 2c and the server machine 2b, and since the HTTP protocol does not make it possible to transmit certificates, the certificate containing precious information is blocked at the level of the security module. The present invention consists of transmitting the certificate from the security module 2c to the server machine 2b in a cookie header of HTTP requests."

Paragraphs [0029] through [0033]; and FIG. 1 (below) of Applicants' published application.

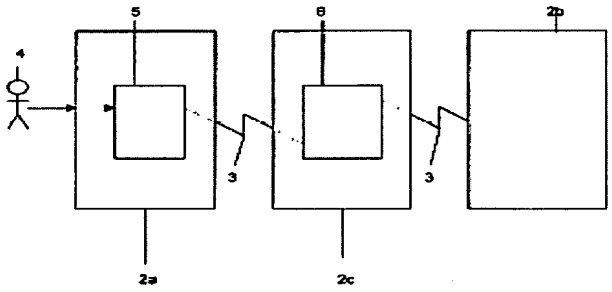


FIG.1

Furthermore, Applicants' disclosure also provides:

"[0044] The user 4 requests access to a page of a given site via the browser 5. The browser 5 sends an HTTP/SSL request through the network 3 to the server machine 2b. The browser 5 requests the universal address (URL--Uniform Resource Locator) of the secure page of the site in question with the prefix "https://". The request, called an access request, is intercepted by the security module 2c, which handles the security services offered by the security protocol used, i.e., in the present example, the SSL protocol. A TCP connection is initialized. The dialog begins with the protocol known as the "handshake," during which a mutual recognition between the user 4 and the security module 2c and an exchange of keys take place."

> "[0045] In the specifications of the SSL protocol, the authentication of the user 4 is optional. In the present invention, the authentication of the user 4 remains optional. If it is required, the analyzing means 6 of the security module 2c request the sending in the "handshake" procedure of a certificate by the client machine 2a. The means 6 transmit the SSL message "CertificateRequest" to the client machine 2a through the network 3."
>
> "[0046] The client machine 2a responds by transmitting the certificate of the user 4 through the network 3 to the security module 2c. The certificate is sent by the machine 2a by means of the SSL "Certificate" message."
>
> "[0047] The module 2c decodes the HTTP message and retrieves the certificate of the user 4 if it has been requested by the module 2c."
>
> "[0048] Once the handshake protocol of the SSL protocol is finished, and if a certificate has been requested and retrieved by the module 2c during the handshake protocol, the analyzing means 6 search the HTTP request for access to the secure page of the site in question sent by the client machine 2a to see if a cookie header exists, i.e., if there is a header entitled "Cookies." In the example illustrated, the header "Cookies" is detected. If no cookie header is present, the analyzing means create a cookie header."

Paragraphs [0044] through [0047] of Applicants' published application (underlines added).

Therefore, Applicants respectfully submit that the claimed security module is sufficiently described in Applicants' disclosure to enable one skilled in the art to make and use the invention of Claims 1-4 and 8-11.

In addition, without acceding to the rejection, Claim 6 has been amended to clarify the subject matter intended to be claimed. For example, Claim 6 now recites, *inter alia*, [a]n apparatus comprising a security machine configured to secure exchanges between a client machine and a server machine of a computer system, in which the security machine further comprises an analyzer configured to insert an unmodified certificate into a cookie header of an HTTP or equivalent request.

Support is provided, for example, at paragraph [0029], [0033], and [0045] of Applicants' published application.

Furthermore, without acceding to the rejection, Claim 7 has also been amended to clarify the subject matter intended to be claimed. For example, Claim 7 now recites, *inter alia*, a system comprising a security module which comprises an analyzer configured to insert an unmodified certificate sent by the client machine into a cookie header of a request in conformance with a non-secure stateless protocol, and in which the analyzer is further configured to transmit to a server said unmodified certificate contained in the cookie header using the non-secure stateless protocol. Support is provided, for example, at paragraph [0029], [0033], and [0045] of Applicants' published application.

In view of the foregoing, Applicants respectfully submit that Applicants' claimed security module, security machine, and analyzer are sufficiently described in Applicants' disclosure to enable one skilled in the art to make and use Applicants' claimed invention. See MPEP §§ 2164.01 and 2164.04; *In re Bowen*, 492 F.3d 859, 862-63 (CCPA 1974).

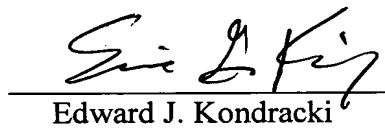
Therefore, Applicants respectfully request that the rejection under § 112 be withdrawn.

Accordingly, Applicants respectfully submit that this application is in condition for allowance. A prompt Notice of Allowance is respectfully requested.

Should the Examiner believe that any further action is necessary to place this application in better form for allowance, the Examiner is invited to contact Applicants' representative at the telephone number listed below.

The Commissioner is hereby authorized to charge to Deposit Account No. 50-1165 (T2147-907679) any fees under 37 C.F.R. §§ 1.16 and 1.17 that may be required by this paper and to credit any overpayment to that Account. If any extension of time is required in connection with the filing of this paper and has not been separately requested, such extension is hereby requested.

Respectfully submitted,

By: 

April 30, 2008

Edward J. Kondracki
Reg. No. 20,604

Eric G. King
Reg. No. 42,736

Miles & Stockbridge, P.C.
1751 Pinnacle Drive
Suite 500
McLean, Virginia 22102-3833
(703) 610-8647
4842-3682-0738